PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification ^{6} :
H04L 29/06

A1

(11) International Publication Number: **WO 96/39769**

(43) International Publication Date: 12 December 1996 (12.12.96)

(21) International Application Number: PCT/US96/04603

(22) International Filing Date: 4 April 1996 (04.04.96)

(30) Priority Data:
08/465,231 5 June 1995 (05.06.95) US

(71) Applicant: SHIVA CORPORATION [US/US]; 28 Crosby Drive, Bedford, MA 01730 (US).

(72) Inventors: RODWIN, Andrew, S.; 126 Box Mill Road, Boxborough, MA 01719 (US). WENOCUR, Jonathan, H.; 140 Kilsyth Road #4, Brighton, MA 02146 (US). FEINSTEIN, Michael, G.; 3 Harvard Drive, Bedford, MA 01730 (US).

(74) Agent: TOSTI, Robert, J.; Testa, Hurwitz & Thibeault, High Street Tower, 125 High Street, Boston, MA 02110-2711 (US).

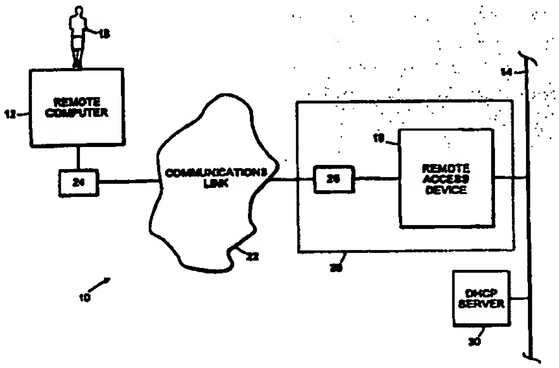
(81) Designated States: AM, AU, AZ, BB, BG, BR, BY, CA, CN, CZ, EE, GE, HU, IS, JP, KG, KP, KR, KZ, LK, LR, LT, LV, MD, MG, MK, MN, MX, NO, NZ, PL, RO, RU, SG, SI, SK, TJ, TM, TR, TT, UA, UZ, VN, ARIPO patent (KE, LS, MW, SD, SZ, UG), European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

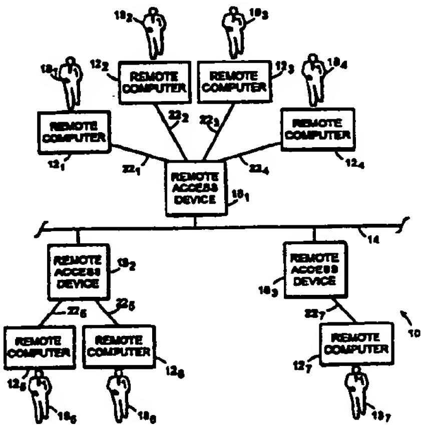
Published
With international search report.

(54) Title: APPARATUS AND METHOD FOR PROVIDING UNIQUE IDENTIFIERS TO REMOTE DIAL-IN NETWORK CLIENTS

(57) Abstract

A remote user (18) at a remote (12) computer accesses a computer network (14) via a remote access device (16) coupled (directly or indirectly) to the network (14). The remote access device receives from the remote computer a request for an identifier. The request does not include any information that uniquely identifies the remote computer or the user thereat. In response to the request, the remote access device generates a client identifier that uniquely identifies the remote computer and then provides that unique client identifier to the remote computer. The remote access device can generate the unique client identifier by concatenating a hardware-level address associated with the remote access device (e.g., a Medium Access Control or MAC address) and the current date and time. The remote computer can store the unique client identifier for future use, and the remote access device can use the unique client identifier to obtain services available on the computer network. For example, the remote access device can use the unique client identifier to identify uniquely the remote computer to a server on the computer network which dynamically assigns Internet Protocol (IP) addresses in order to obtain an IP address for the remote computer.





FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AM	Armenia
AT	Austria
AU	Australia
BB	Barbados
BE	Belgium
BF	Burkina Faso
BG	Bulgaria
BJ	Benin
BR	Brazil
BY	Belarus
CA	Canada
CF	Central African Republic
CG	Congo
CH	Switzerland
CI	Côte d'Ivoire
CM	Cameroon
CN	China
CS	Czechoslovakia
CZ	Czech Republic
DE	Germany
DK	Denmark
EE	Estonia
ES	Spain
FI	Finland
FR	France
GA	Gabon
GB	United Kingdom
GE	Georgia
GN	Guinea
GR	Greece
HU	Hungary
IE	Ireland
IT	Italy
JP	Japan
KE	Kenya
KG	Kyrgystan
KP	Democratic People's Republic of Korea
KR	Republic of Korea
KZ	Kazakhstan
LI	Liechtenstein
LK	Sri Lanka
LR	Liberia
LT	Lithuania
LU	Luxembourg
LV	Latvia
MC	Monaco
MD	Republic of Moldova
MG	Madagascar
ML	Mali
MN	Mongolia
MR	Mauritania
MW	Malawi
MX	Mexico
NE	Niger
NL	Netherlands
NO	Norway
NZ	New Zealand
PL	Poland
PT	Portugal
RO	Romania
RU	Russian Federation
SD	Sudan
SE	Sweden
SG	Singapore
SI	Slovenia
SK	Slovakia
SN	Senegal
SZ	Swaziland
TD	Chad
TG	Togo
TJ	Tajikistan
TT	Trinidad and Tobago
UA	Ukraine
UG	Uganda
US	United States of America
UZ	Uzbekistan
VN	Viet Nam

APPARATUS AND METHOD FOR
PROVIDING UNIQUE IDENTIFIERS TO REMOTE DIAL-IN NETWORK CLIENTS

Field of the Invention

This invention relates to providing remote users at remote computers with access to a local computer network, and more particularly, to providing each remote dial-in client dynamically and automatically with an identifier that uniquely identifies the client on the network.

Background of the Invention

The client-server computer networking model allows organizations of all sizes to utilize group productivity products such as e-mail. Many business organizations have grown to rely heavily on network services. Employees who travel typically need to access the same network services and resources provided to them at work. Field offices also frequently need to access the headquarters' network services. The term "telecommuter" has been used to describe an employee who stays at home and conducts business by accessing the network services provided at the traditional worksite. These types of users are sometimes referred to as "remote" or "remote clients" because they typically are located in a physically remote place from the networks and because they do not connect to the networks locally or directly. Remote users typically connect to the networks via telephone lines. The terms "remote access" and "remote networking" are frequently used to identify the situation in which a remote user accesses a computer network over analog or digital telephone lines.

A remote user generally can utilize any type of computer to access the network. The client computer can be, for example, a personal computer, a workstation, or a portable computer such as a laptop computer, a notebook computer, or a palmtop computer. Also, the computer can be, for example, an IBM PC or compatible, an Apple Macintosh, or a Unix-based computer. The user typically connects a modem (or other communications adapter such as a digital adapter if the telephones lines are wholly digital) to a serial port of the computer. The modem (or other communications adapter) connected to the user's remote computer communicates over the telephone lines with another modem (or other communications adapter) which is coupled to a device coupled to the network. The other modem (or other communications adapter) and the device are located at the network which the remote client is attempting to access. The device can be coupled directly to the network, or it can be coupled to the network which the remote client is attempting to access via a communications link (e.g., a WAN link) to that network. It is this device which provides the remote computer with controlled access to the network and the services and resources thereon. The device typically is referred to as a "remote access server" or a "remote access device," and it generally includes at least one serial port for connecting to the other modem, at least one port for connecting to the network, and electronics which include at least a microprocessor and memory. A typical remote access device provides a point of network access for one or more remote clients.

It can be useful for each participant communicating on or attempting to access the network, including remote clients dialed or dialing into the network via one or more remote access devices, to be uniquely identifiable on the network. For example, if a dynamic internet protocol (IP) address assignment/management server (e.g., a DHCP or Dynamic Host Configuration Protocol server) coupled to the network (directly or via a communications link such as a WAN link) can uniquely identify each remote client, each remote client can be dynamically assigned the same IP address even if the user disconnects from the network and then later reconnects, via the same or a different remote access device, before the dynamically-assigned, server-supplied IP address lease expires. (With some network protocols such as TCP/IP, any network participant, including a remote client which dials into the network, requires an IP address to communicate on the network and utilize the various network services.) However, while it can be useful and desirable to identify uniquely each network participant, it generally is not known how to accomplish this result dynamically for remote clients dialed into the network via remote access devices without individually serializing each remote client ahead of time such that each already has a unique identifier.

For nodes coupled to the network, it is known to use as the unique identifier a hardware-level address associated with each such node (e.g., the MAC address on the network interface card of each network node). However, this hardware-level address is not useful as a unique identifier for remote computers because each remote access device coupled to the network (directly or indirectly via a communications link such as a WAN link) typically has more than one remote computer dialed thereinto. That is, the single hardware-level address of a remote access device is insufficient to identify uniquely each of the remote clients accessing the network via that one remote access device. The tendency of some users to utilize the exact same username (e.g., "Joe" or "Smith") renders the username a poor choice as a unique identifier for each network participant.

A simple and reliable way of dynamically providing a unique identifier to each network participant, including remote clients accessing the network via dial-in connections to remote access devices coupled to the network (directly or indirectly via a communications link such as a WAN link), is needed.

Summary of the Invention

It is an object of this invention to allow one or more remote users at remote computers (i.e., one or more remote clients) to dial-in and gain access to a local computer network via a remote access device coupled to the network.

It is another object of the invention to identify uniquely on the network each of the remote clients dialed thereinto via remote access devices.

It is a further object of the invention to provide each remote dial-in client dynamically and automatically with an identifier uniquely identifying the client on the network that the client is dialing into via a remote access device. The unique identifier is provided to the remote dial-in client even though the client initially does not, and/or is not able to, provide unique information about the remote computer and/or the remote user thereat to the remote access device or the network. With its dynamically provided unique identifier, the client can then use the unique identifier to access various network services available on the network. For example, the client can then obtain an internet protocol (IP) address dynamically from a Dynamic Host Configuration Protocol (DHCP) server coupled to the network.

The invention does not rely on usernames to identify uniquely the remote clients or to generate the unique identifiers, and therefore remote users are allowed to share usernames.

In general, the invention involves a remote user at a remote computer (i.e., a remote client) dialing into a computer network via a remote access device coupled to the network. The remote computer includes software which aids the remote user in dialing into the remote access device (and thus the network) over, for example, the public telephone lines. If an identifier is already stored in the remote computer, that identifier is automatically sent to the remote access device. If an identifier is however not yet stored at the remote computer (because, for example, this is the first time the remote client has tried to access the network), the remote computer automatically requests an identifier from the remote access device. The remote access device receives the request and then provides to the remote client an identifier guaranteed to be universally unique on the network. This unique identifier is stored by the remote computer. The remote client can use the identifier to obtain network services. For example, the identifier can be used by the remote access device to identify uniquely the remote client to a DHCP server to obtain an IP address for the client.

After the remote client eventually disconnects from the remote access device (and thus disconnects from the network), that client can later reconnect to the same or a different remote access device to again access the network. Upon reconnection, the remote computer automatically retrieves the stored unique identifier and passes it to the remote access device. Because the unique identifier is stored by the remote computer, access to the network can be accomplished via the same pre-disconnection remote access device or a different remote access device coupled to the network. The remote access device can then use the unique identifier to obtain network services. For example, the remote access device can use the identifier to obtain from the same DHCP server the same IP address for the client as was obtained during the previous dial-in connection.

In a preferred embodiment of the invention, after receiving the request for an identifier from a remote computer dialed thereinto, the remote access device generates a unique identifier by concatenating two items: (1) a hardware-level address associated with the remote access device, preferably the MAC address on a network interface card that the remote access device uses to couple to the network; and (2) the current date and time which preferably is derived from an on-board Real Time Clock chip in the remote access device. Since the MAC address of a node coupled to the network is by definition globally unique on the network and in the world, and because the date and time is guaranteed to be unique at any particular instant, the concatenation of these two items is guaranteed to yield a globally unique identifier even if more than one client is dialed into the same remote access device. While it is unlikely that two or more remote clients will dial into the same remote access device and request an identifier at precisely the same instant in time or even within a short interval of time (e.g., one second), the remote access device avoids any such conflict by storing the last identifier generated and provided to a remote computer and making sure that the current identifier contains a date/time value different (e.g., greater) than the last identifier before providing the current identifier to a remote computer.

The invention provides remote dial-in clients with unique identifiers even if the clients initially do not, and/or are not able to, provide uniquely identifying information about themselves to either the remote access device or the network. For example, in a situation where an Internet Access Provider (IAP) offers free trial service by distributing (e.g., with a magazine) identical computer disks to potential customers, the invention is useful for generating and utilizing unique identifiers for each potential customer who loads the software on the disk into his or her computer and attempts to take advantage of the free trial Internet access. In such a mass distribution, the disks typically are identical and they contain no unique information. That is, the software on each of the disks contains no information that distinguishes it from any of the other disks. The cost of producing the disks increases if, instead of being identical, each of the disks is coded with some unique identifying information such as a unique serial number. Since the disks are completely identical, the remote clients have no way of identifying themselves uniquely to the remote access device to which they dial into to access the network. In accordance with the invention, unique identifiers can be generated dynamically and automatically by the remote access device and then provided to the clients dialed thereinto.

The foregoing and other objects, aspects, features, and advantages of the invention will become more apparent from the following description and from the claims.

Brief Description of the Drawings

In the drawings, like reference characters generally refer to the same parts throughout the different views. Also, the drawings are not necessarily to scale, emphasis instead generally being placed upon illustrating the principles of the invention.

FIG. 1A is a simplified diagram of a remote access system in which a remote access device according to the invention provides a remote user at a remote computer with access to a local computer network.

FIG. 1B is a diagram of a remote access system having a plurality of remote access devices and a plurality of remote users at a plurality of remote computers.

FIG. 2 is a diagram of a remote access system shown in more detail than the system shown in FIG. 1A.

FIG. 3A is a flowchart for providing a unique client identifier to a remote dial-in network client according to the invention.

FIGS. 3B and 3C are flowcharts showing some details of the operations of FIG. 3A.

FIG. 4 is a block diagram showing major components of a remote access device according to the invention.

Description

Referring to FIG. 1A, in a remote access system 10, a remote computer 12 is allowed access to a local computer network 14 by a remote access device 16. As will be described in more detail later with reference to FIGS. 1B and 3, the remote access device 16 is itself a powerful programmable computer which provides a point of network access for one or more remote users/computers 18,12. A remote user at a remote computer generally is referred to herein as a remote client. Only one remote user 18 and one remote computer 12 is shown in FIG. 1A for simplicity. In some embodiments, the remote access device 16 is a LanRover which is available from Shiva Corporation of Burlington, MA. In some other embodiments, the device 16 can be a NetModem/E or other platforms available from Shiva Corporation.

The remote user 18 at the remote computer 12 initiates an attempt to gain access to the network 14 (and the network services and resources available thereon such as a dynamic Internet Protocol (IP) address assignment/management server like a Dynamic Host Configuration Protocol, DHCP, server 30) via the remote access device 16 by dialing into the device 16 over telephone lines 22. The term telephone lines 22 is used herein to mean any digital and/or analog communication link or links used to transmit voice and/or data including wireless links and cellular data links such as Cellular Digital Packet Data (CDPD).

In the disclosed embodiment, a modem 24 is connected to the remote computer 12, and another modem 26 is connected to the remote access device 16. The modems 24, 26 allow the remote computer 12 and the remote access device 16 to communicate over the telephone lines 22. Note that the modem 26 connected to the remote access device 16 could be part of the remote access device 16 (e.g., included within the device's housing), as indicated by the dotted-line box 28 enclosing the remote access device 16 and the modem 26 connected thereto. Also note that the modems 24, 26 could be Integrated Services Digital Network (ISDN) terminal adapters if the telephone lines 22 are the ISDN, or the modems 24, 26 could be any of a variety of other switched-access devices.

Referring to FIG. 1B, the remote access system 10 can include one or more remote clients dialed into a single remote access device 16. While one of the remote access devices is shown with four remote clients dialed thereinto, another remote access device is shown with two clients dialed thereinto, and another has one client dialed thereinto, it generally is possible to have any number of remote clients dialed into any particular remote access device. In some embodiments, a remote access device according to the invention allows up to eight remote clients to dial into the network via the device. In some other embodiments, the device allows sixteen or more clients to dial into the network.

Referring to FIG. 2, the remote access system 10 of FIG. 1A is shown in more detail. The remote computer 12 is a portable laptop computer. In general, the remote computer 12 can be any type of portable computer (e.g., a laptop, a notebook, or a palmtop), workstation, or personal computer (e.g., an IBM PC or compatible, an Apple Macintosh, or a Unix-based computer). The remote computer 12 generally must be able to function as a stand-alone computer system when not connected to a network, and as a full network node when it is dialed-in to the network 14 through the remote access device 16. For a remote Macintosh system, it generally is preferred that the computer have at least a 25 MHz 68030 processor. For a remote PC system, it generally is preferred that the computer have at least a 25 MHz 486 processor.

In general, the remote computer 12 of the remote access system 10 must have enough processing power, internal memory, and storage (e.g., disk, tape, etc.) space to run, on the remote computer 12 itself, the remote user's chosen applications without relying upon the on-network communication speed which typically is much higher than the speed of the telephone line link 22. Some telephone lines 22 allow speeds of up to 57.6 or 115.2 kilobits per second whereas the local computer network 14 can operate in ranges from 1 to 100 megabits per second depending on the type of network. The local computer network 14 can be, for example, Ethernet or Token Ring.

The remote computer 12 typically will have a serial port 32 which is managed by a serial controller such as a 16550A serial controller chip which can receive or transmit up to sixteen characters without intervention from the central processing unit (CPU) of the remote computer 12. The modem 24 connected to the serial port 32 can be, for example, a V.34 modem (28.8 kilobits per second) or an ISDN terminal adapter. The other modem 26 (which is not shown in FIG. 2 because it is internal to the remote access device 16) is selected to operate properly given the telephone lines 22 employed and the modem 24 connected to the serial port 32.

The network services and resources available on the network 14 which the remote user 18 might access via the remote access device 16 can include, for example, a Notes Server 46 and an E-Mail Server 48 in addition to the DHCP server 30.

The remote computer 12 can be loaded with network application software 34 and remote access client software 36. The remote access client software 36 can allow, as a relevant example, a Unix-based computer to use a standard Point-to-Point Protocol (PPP) implementation, and a PC-based computer to use any standard (if any) or vendor-supplied remote access clients. A remote access client includes a "dialer" which establishes and terminates the remote access connection and a "driver" which interfaces with the network protocol stacks and the serial port 32 to send and receive network data. The remote access client can operate with a variety of protocols including IPX, TCP/IP, NetBEUI, LLC/802.2, and AppleTalk. Novell's IPX is the native protocol for NetWare. TCP/IP is widely used in Unix-based systems and client-server databases, and TCP/IP also is becoming standard for many other applications. NetBEUI is used for LAN Manager and Microsoft's Windows for Workgroups. LLC/802.2 is for IBM LAN Server and host connectivity. The combination of AppleTalk and TCP/IP covers almost all Macintosh applications.

The remote access client software 36 can be, for example, supplied on a computer disk provided free of charge by an Internet Access Provider (IAP). The IAP may be offering a free trial Internet connection by distributing (e.g., with a magazine) identical computer disks to potential customers. A potential customer loads the free disk into his or her computer to take advantage of the free trial Internet access. The software on the free disk helps to establish a free trial connection to the Internet via the phone lines. In such a mass distribution, the disks typically are identical and they contain no unique information. That is, the software on each of the disks contains no information that distinguishes it from any of the other disks. The cost of producing the disks increases if, instead of being identical, each of the disks is coded with some unique identifying information such as a unique serial number. Since the disks are completely identical, the remote clients have no way of identifying themselves uniquely to the remote access device to which they dial into to access the Internet for the free trial. In accordance with the invention, unique identifiers can be generated dynamically and automatically by the remote access device and then provided to the clients dialed thereinto.

As an aside, IAPs offer direct connection to the Internet, as opposed to traditional on-line time-sharing services that only provide limited, controlled Internet access via the service's computer which is connected to the Internet. Examples of IAPs are Performance Systems International (PSINet®), Inc. (510 Huntmar Park Drive, Herndon, VA 22070, (703) 709-0300 or (800) 827-7482) and MASSinternet ((800) 236-9737)). Examples of traditional on-line time-sharing services are Prodigy, Compuserve, and America Online.

Referring to FIG. 3A, in accordance with the invention, a remote user 18 at a remote computer 12 (i.e., a remote client) dials into a remote access device 16 in an attempt to connect to a computer network 14 (step 50). The remote access device 16 is coupled to the computer network 14 either directly as shown or indirectly via a communications link such as a WAN link. The remote computer 12 includes remote access client software 36 (e.g., free software provided by an IAP as described previously) which aids the remote client in dialing into the remote access device 16 (and thus the network 14) over the public telephone lines 22. If an identifier is already stored in the remote computer 12 (decision box 52), that identifier is automatically sent to the remote access device 16 in order to obtain network services via the remote access device 16 (steps 54 and 62). If an identifier is however not yet stored at the remote computer 12 (because, for example, this is the first time the remote client has tried to access the network), the remote computer 12 automatically requests an identifier from the remote access device 16 (step 56). In accordance with the invention, neither the remote access client software 36 nor the request sent by the remote computer 12 to the remote access device 16 includes any uniquely identifying information. That is, the remote access device 16 does not receive any information uniquely identifying the remote computer 12 or the remote user thereat. The remote access device 16 receives the request and then generates and provides to the remote client an identifier guaranteed to be universally unique on the network 14 (step 58). In the disclosed embodiment, the request sent by the remote computer 12 is in the form of a "null" identifier, and the remote access device 16 interprets this "null" identifier as an indication that it should generate and assign to the client a new unique client identifier. The unique client identifier is stored by the remote computer 12 (step 60). For example, the remote computer can store the unique client identifier in a file (e.g., an initialization file) on its hard disk. The remote client can now use this unique client identifier to obtain network services via the remote access device 16 (step 62). For example, the identifier can be used by the remote access device to identify uniquely the remote client to a DHCP server to obtain dynamically an IP address for the client.

If (or when) the remote client disconnects or is disconnected from the remote access device 16 and thus disconnects or is disconnected from the network 14 (step 64), that client can later reconnect to the same or a different remote access device to again access the network 14 (step 50). Upon reconnection (step 50), the remote computer 12 automatically retrieves the stored unique client identifier stored thereat (decision box 52) and passes it to the remote access device (step 54) in order to again obtain network services (step 62). Because the unique client identifier is stored by the remote computer 12, access to the network 14 can be accomplished via the same pre-disconnection remote access device (16_1) or a different remote access device (16_2) coupled (directly or indirectly) to the network 14. The remote access device can then use the unique client identifier to obtain network services. For example, the remote access device can use the unique client identifier to obtain from the DHCP server the same IP address for the client as was obtained during the previous dial-in connection.

Note that this exchange of identifier information is not meant to replace authentication of the client. If it were to be used for authentication, it would have to be subject to some randomization technique used to prevent recording and playback.

Referring to FIGS. 3B and 3C, in the disclosed embodiment of the invention, after receiving the request for an identifier from the remote computer dialed thereinto, the remote access device generates the unique client identifier (step 58) by concatenating two items (step 66). The two items are: (i) a hardware-level address associated with the remote access device, such as the MAC address on a network interface card that the remote access device uses to couple (directly or indirectly) to the network 14; and (ii) the current date and time which preferably is derived from an on-board Real Time Clock chip in the remote access device. Since the MAC address of a node coupled (directly or indirectly) to the network is by definition globally unique on the network 14 and in the world, and because the date and time is guaranteed to be unique at any particular instant, the concatenation of these two items is guaranteed to yield a globally unique identifier even if more than one client is dialed into the same remote access device.

While it is unlikely that at precisely the same instant in time, or even within a short interval of time (e.g., one second), two or more remote clients will dial into the same remote access device and request an identifier, the remote access device avoids any such conflict by storing the last identifier generated and provided to a remote computer (step 68) and checking or comparing the stored identifier against the most recently generated (current) identifier to make sure that the current identifier contains a date/time value different (e.g., greater) than the stored identifier before providing the current identifier to a remote computer (step 70). If the current identifier is not different than stored identifier (decision box 72), discard the current identifier and generate another identifier to replace it (step 74). This replacement identifier then becomes the current identifier, and the comparison with the stored identifier is performed again (step 70). If the current and stored identifiers are different, the current identifier becomes the stored identifier (e.g., the value in storage is overwritten with the current identifier), and the current identifier is provided to the remote computer (step 76).

Note that the above-described identifier generation technique assumes or requires that the remote access server's date and time is correct. In general, measures must be taken to ensure the correctness of the date and time. These measures can include making sure that the Time Server(s) on the network from which the remote access devices obtain time/date information are accurate and/or prompting the network administrator to check the remote access devices' date and time at certain points.

The invention thus provides remote dial-in clients with unique identifiers even though the clients initially do not provide uniquely identifying information about themselves to either the remote access device or the network. The invention does not rely on usernames to identify uniquely the remote clients or to generate the unique client identifiers, and therefore remote users are allowed to share usernames.

Further details about the remote access device according to the invention are provided below.

The performance of the remote access device 16 is primarily determined by the ability to move data through its serial ports without much attention from its CPU. The performance of the remote access device 16 also is determined by its CPU's ability to perform the routing, filtering, IP address tracking, etc. that the CPU must do without adding undue delays as it forwards data packets. The remote access device 16 thus has generally been optimized for serial port throughput and general CPU power. Because the remote access device 16 must be highly reliable and efficient, it includes solid-state, non-volatile storage for the controlling software. The software is upgradeable via downloading from the network 14 to the remote access device 16. The network manager can perform any upgrades.

In general, the software in the remote access device 16 causes the remote access device 16 to perform the functionality described herein, although it should be noted that it is possible to use dedicated electronic hardware to perform all of the functionality described herein.

FIG. 4 shows one embodiment of the remote access device 16. Other embodiments have different configurations. Referring to FIG. 4, one embodiment of the remote access device 16 includes electronics 38, a plurality of serial communication ports 40_1-40_N, and a plurality of network ports 42_1-42_M. The remote access device 16 also can include a plurality of internal modems 44_1-44_N. The serial ports 40 and the network ports 42 are controlled by the electronics 38.

The electronics 38 include, in some embodiments, a powerful 25 MHz 68EC020 microprocessor and memory such as one or more (e.g., two) megabytes of battery backed-up static random access memory (SRAM) and 64 kilobytes in an erasable programmable read only memory (EPROM). The electronics 38 also can include an on-board Real Time Clock chip 39 from which the remote access device 16 can obtain date and time information.

Each of the serial communication ports 40 is for coupling with a communication device (e.g., the modem 26 of FIG. 1A), or for coupling with the telephone lines 22, to provide for communication with a remote computer (e.g., the remote computer 12 of FIGS. 1 and 2) over the telephone lines 22. A connecting cable can be used to couple a serial port 40 with the communication device or with the telephone lines. Each of the serial ports 40 can simultaneously be coupled to a different one of the one or more remote computers so as to provide simultaneous access to the local computer network 14 for each of the remote computers, even if each of the remote computers employs a different protocol (e.g., IPX, TCP/IP, AppleTalk, NetBEUI, or 802.2/LLC). In some embodiments, the remote access device 16 includes eight serial ports 40, each port 40 being a DB-25 asynchronous serial port which supports speeds of up to 115.2 kilobits per second (kbps), with an internal V.34 modem 44 associated with each.

Each of the network ports 42 is for coupling with a local computer network (e.g., the network 14 of FIGS. 1 and 2), via a connecting cable, to provide for communication with the network. Typically, the remote access device 16 is connected to only one network during normal operation, although it is possible with some embodiments to connect to more than one network. In some embodiments, the remote access device 16 includes three network ports 42, one for 10BaseT Ethernet, one for Thin Ethernet, and one for Thick Ethernet. In some other embodiments, the remote access device 16 includes a single network port 42 for Token Ring. In general, the network ports 42 are network interface cards and each has a hardware-level address thereon such as a Medium Access Control (MAC) address.

The remote access device 16 shown functionally in FIG. 4 can be contained in a housing similar to that shown in FIG. 2. The housing preferably is less than or equal to about 1.7 by 17 by 10 inches. Other housing sizes are possible. The housing can be made rack-mountable.

Variations, modifications, and other implementations of what is described herein will occur to those of ordinary skill in the art without departing from the spirit and the scope of the invention as claimed. Accordingly, the invention is to be defined not by the preceding illustrative description but instead by the following claims.

What is claimed is:

Claims

1. A method for providing unique identifiers to remote computers, comprising:

providing a remote access device coupled to a computer network;

receiving at the remote access device a request for an identifier from a remote computer which is attempting to gain access to the computer network via the remote access device which is located remote from the remote computer as is the computer network;

generating at the remote access device a unique client identifier in response to the request for the identifier received from the remote computer, the unique client identifier uniquely identifying the remote computer; and

providing the unique client identifier to the remote computer.

2. The method of claim 1 further comprising:

storing the unique client identifier at the remote computer; and

using the unique client identifier to obtain services available on the computer network.

3. The method of claim 2 wherein the step of using the unique client identifier comprises the remote access device using the unique client identifier to identify uniquely the remote computer to a server on the computer network which dynamically assigns internet protocol (IP) addresses in order to obtain an IP address for the remote computer.

4. The method of claim 1 wherein the step of receiving the request comprises receiving the request which does not include any information uniquely identifying the remote computer or a user at the remote computer.

5. The method of claim 1 wherein the step of generating the unique client identifier comprises:

concatenating a hardware-level address associated with the remote access device and the current date and time.

6. The method of claim 5 wherein the step of concatenating comprises concatenating a Medium Access Control (MAC) address associated with the remote access device and the current date and time.

7. A method for providing unique identifiers to remote computers, comprising:

providing a remote access device coupled to a computer network at a first location;

providing a remote computer at a second location remote from the first location;

receiving at the remote access device a request for an identifier from the remote computer which is attempting to gain access to the computer network via the remote access device, the request including no information uniquely identifying the remote computer or a user at the remote computer;

generating at the remote access device a unique client identifier in response to the request for the identifier received from the remote computer, the unique client identifier uniquely identifying the remote computer;

providing the unique client identifier to the remote computer; and

using the unique client identifier to obtain services available on the computer network.

8. The method of claim 7 further comprising:

storing the unique client identifier at the remote computer.

9. The method of claim 7 wherein the step of using the unique client identifier comprises the remote access device using the unique client identifier to identify uniquely the remote computer to a server on the computer network which dynamically assigns internet protocol (IP) addresses in order to obtain an IP address for the remote computer.

10. The method of claim 7 wherein the step of generating the unique client identifier comprises:

concatenating a hardware-level address associated with the remote access device and the current date and time.

11. The method of claim 10 wherein the step of concatenating comprises concatenating a Medium Access Control (MAC) address associated with the remote access device and the current date and time.

12. Apparatus for providing unique identifiers to remote computers, comprising:

a computer network located at a first location;

a remote computer at a second location remote from the first location; and

a remote access device, coupled to the computer network at the first location, comprising means for receiving a request for an identifier from the remote computer which is attempting to gain access to the computer network via the remote access device, the request including no information uniquely identifying the remote computer or a user at the remote computer,

means for generating a unique client identifier in response to the request for the identifier received from the remote computer, the unique client identifier uniquely identifying the remote computer,

means for providing the unique client identifier to the remote computer, and

means for using the unique client identifier to obtain services available on the computer network.

13. The apparatus of claim 12 wherein the remote computer comprises means for storing the unique client identifier.

14. The apparatus of claim 12 wherein the means for using the unique client identifier comprises means for using the unique client identifier to identify uniquely the remote computer to a server on the computer network which dynamically assigns internet protocol (IP) addresses in order to obtain an IP address for the remote computer.

15. The apparatus of claim 12 wherein the means for generating the unique client identifier comprise means for concatenating a hardware-level address associated with the remote access device and the current date and time.

16. The apparatus of claim 15 wherein the means for concatenating comprise means for concatenating a Medium Access Control (MAC) address associated with the remote access device and the current date and time.

17. Apparatus for providing unique identifiers to remote computers, comprising:

a communications link;

a remote computer, at a first location, for sending a request for an identifier over the communications link, the request including no information uniquely identifying the remote computer or a user at the remote computer;

a computer network located at a second location remote from the first location; and

a remote access device, coupled to the computer network at the second location, for receiving the request from the communications link, generating in response to the request a unique client identifier which uniquely identifies the remote computer, and providing the unique client identifier to the remote computer.

18. The apparatus of claim 17 wherein the remote computer comprises means for storing the unique client identifier.

19. The apparatus of claim 17 wherein the remote access device also uses the unique client identifier to obtain, for the remote computer, services available on the computer network.

20. The apparatus of claim 19 wherein the remote access device uses the unique client identifier to identify uniquely the remote computer to a server on the computer network which dynamically assigns internet protocol (IP) addresses in order to obtain an IP address for the remote computer.

21. The apparatus of claim 17 wherein the remote access device generates the unique client identifier by concatenating a hardware-level address associated with the remote access device and the current date and time.

22. The apparatus of claim 21 wherein the remote access device concatenates a Medium Access Control (MAC) address associated with the remote access device and the current date and time.

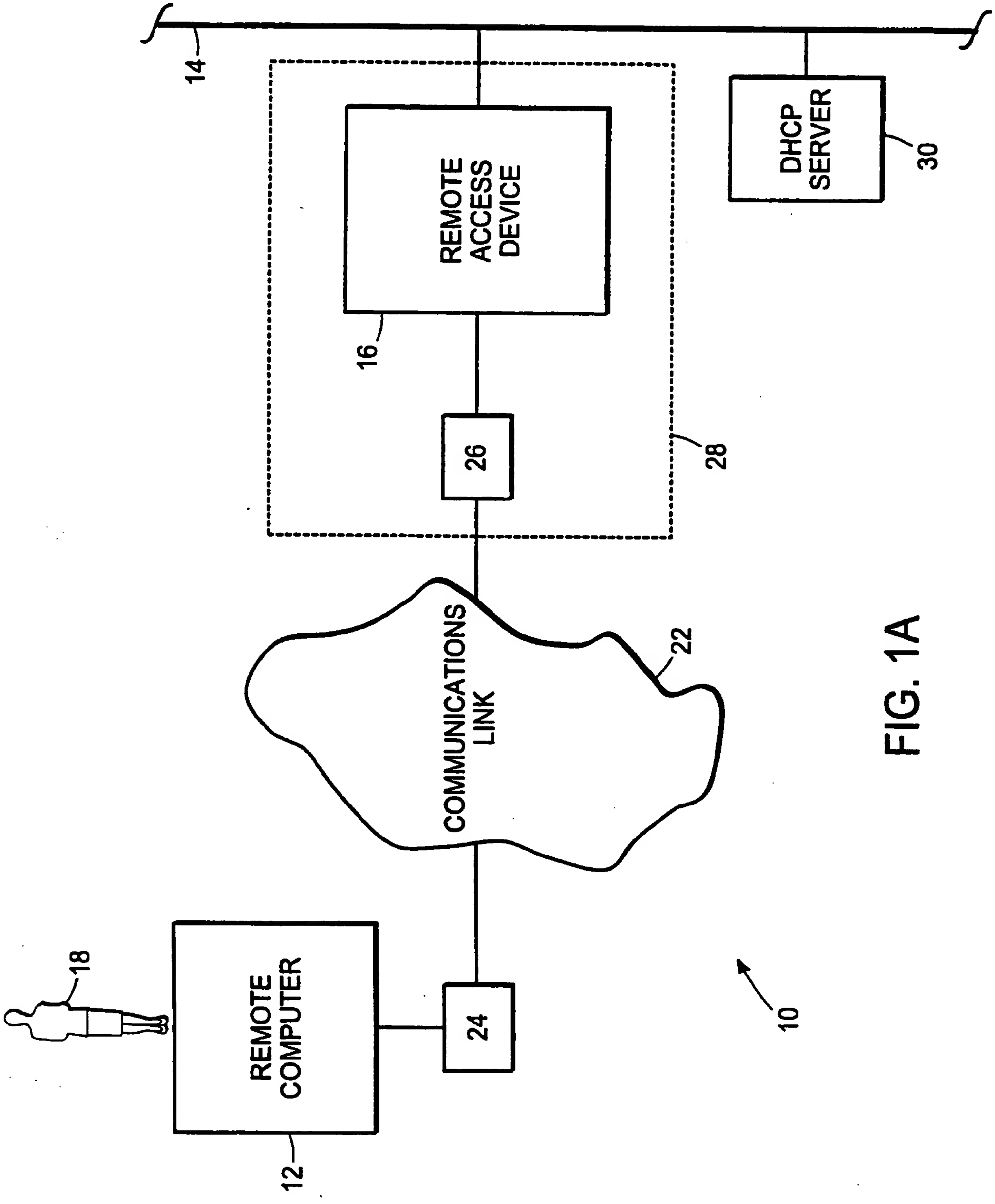

14
REMOTE ACCESS DEVICE
16
26
28
DHCP SERVER
30
COMMUNICATIONS LINK
22
REMOTE COMPUTER
12
18
24
10

FIG. 1A

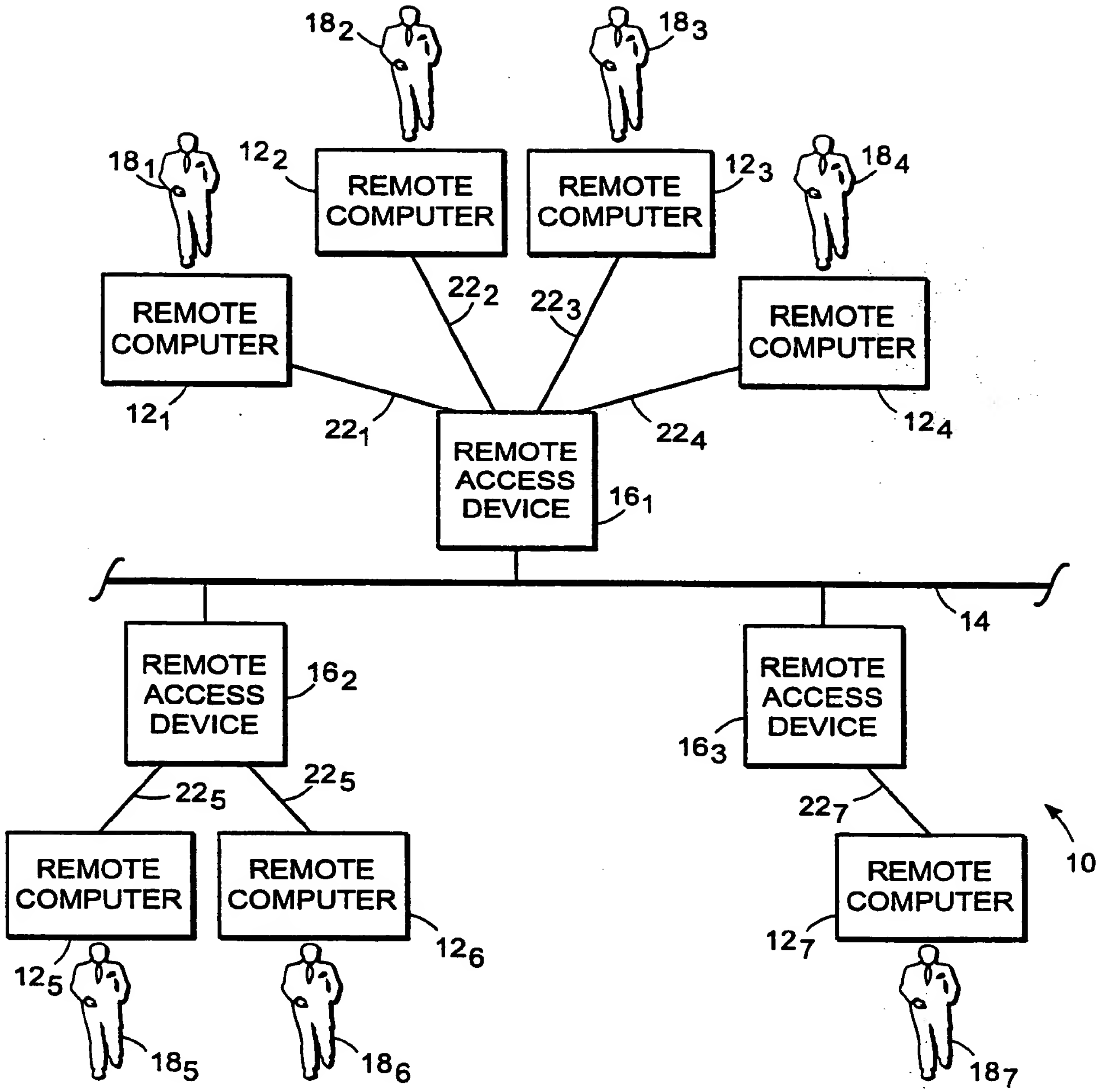

18_2
18_3
18_1
12_2
REMOTE COMPUTER
REMOTE COMPUTER
12_3
18_4
REMOTE COMPUTER
22_2
22_3
REMOTE COMPUTER
12_1
22_1
REMOTE ACCESS DEVICE
22_4
12_4
16_1
14
REMOTE ACCESS DEVICE
16_2
REMOTE ACCESS DEVICE
16_3
22_5
22_5
22_7
10
REMOTE COMPUTER
REMOTE COMPUTER
REMOTE COMPUTER
12_6
12_7
12_5
18_5
18_6
18_7

FIG. 1B

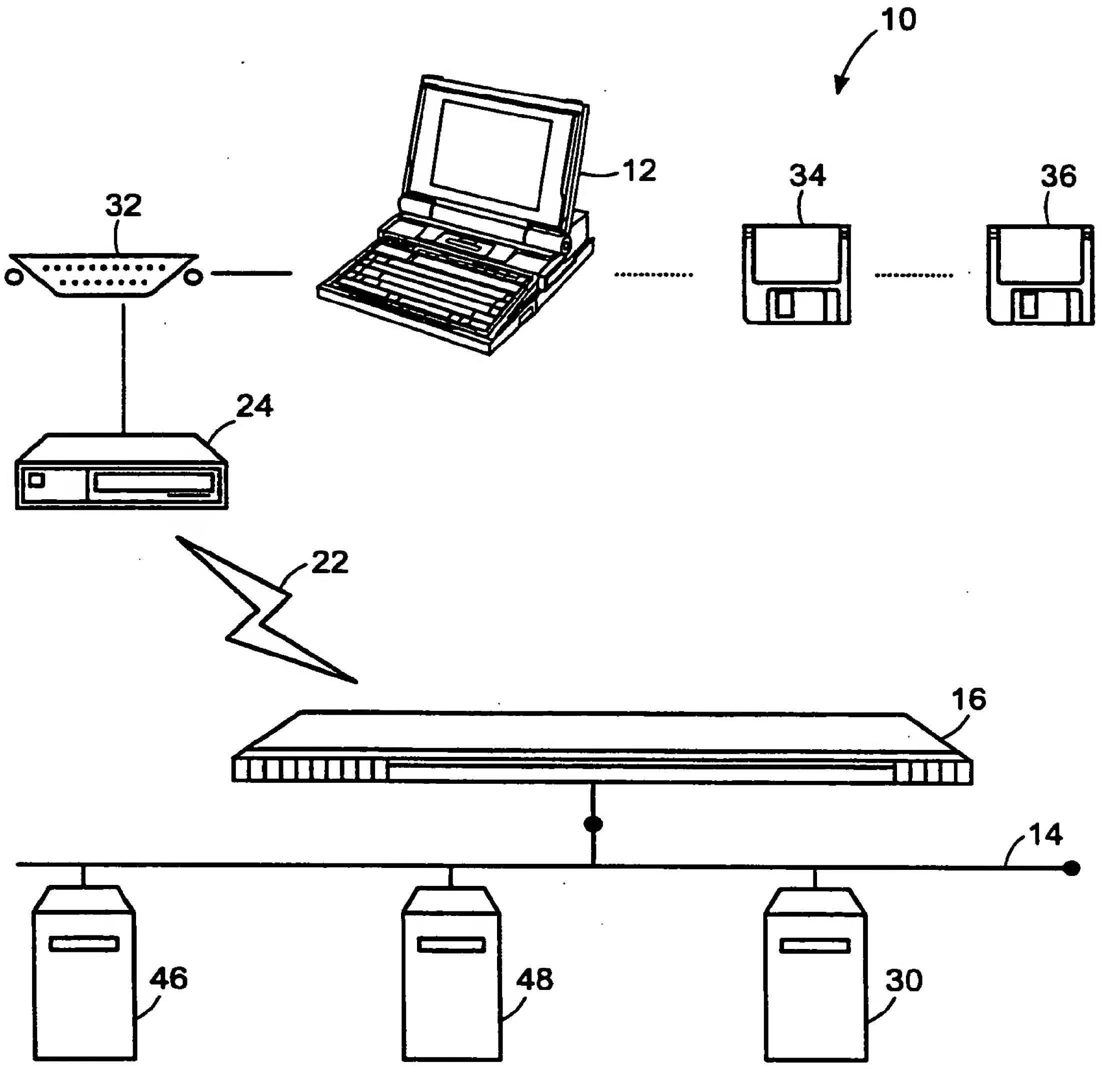


FIG. 2

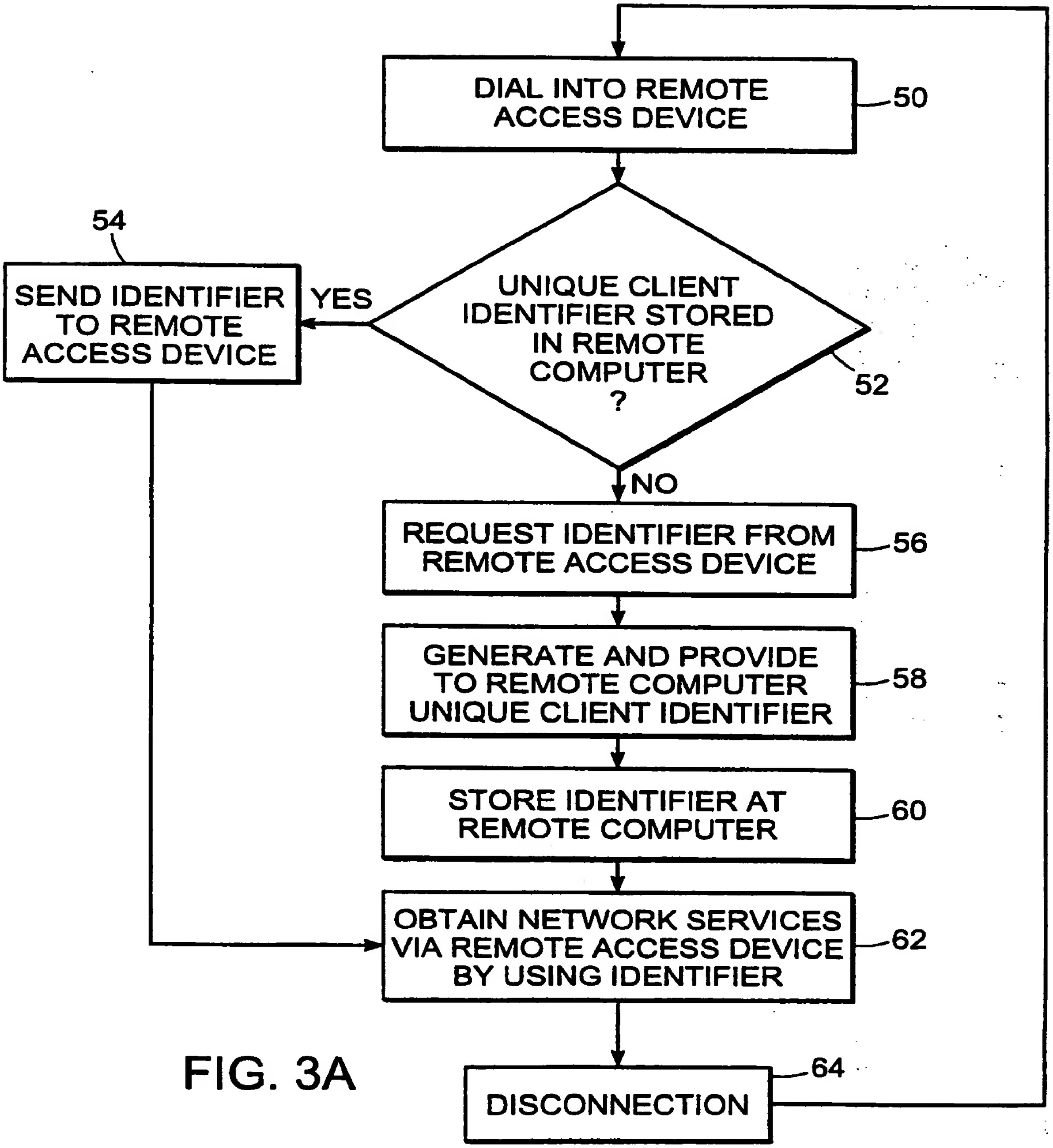

DIAL INTO REMOTE ACCESS DEVICE
50
UNIQUE CLIENT IDENTIFIER STORED IN REMOTE COMPUTER ?
52
YES
SEND IDENTIFIER TO REMOTE ACCESS DEVICE
54
NO
REQUEST IDENTIFIER FROM REMOTE ACCESS DEVICE
56
GENERATE AND PROVIDE TO REMOTE COMPUTER UNIQUE CLIENT IDENTIFIER
58
STORE IDENTIFIER AT REMOTE COMPUTER
60
OBTAIN NETWORK SERVICES VIA REMOTE ACCESS DEVICE BY USING IDENTIFIER
62
DISCONNECTION
64

FIG. 3A

FIG. 3B

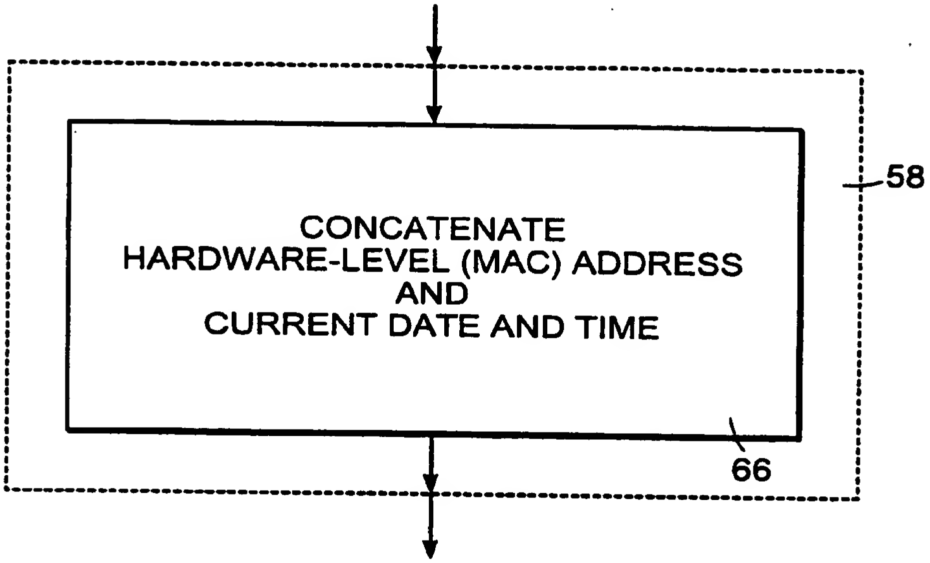
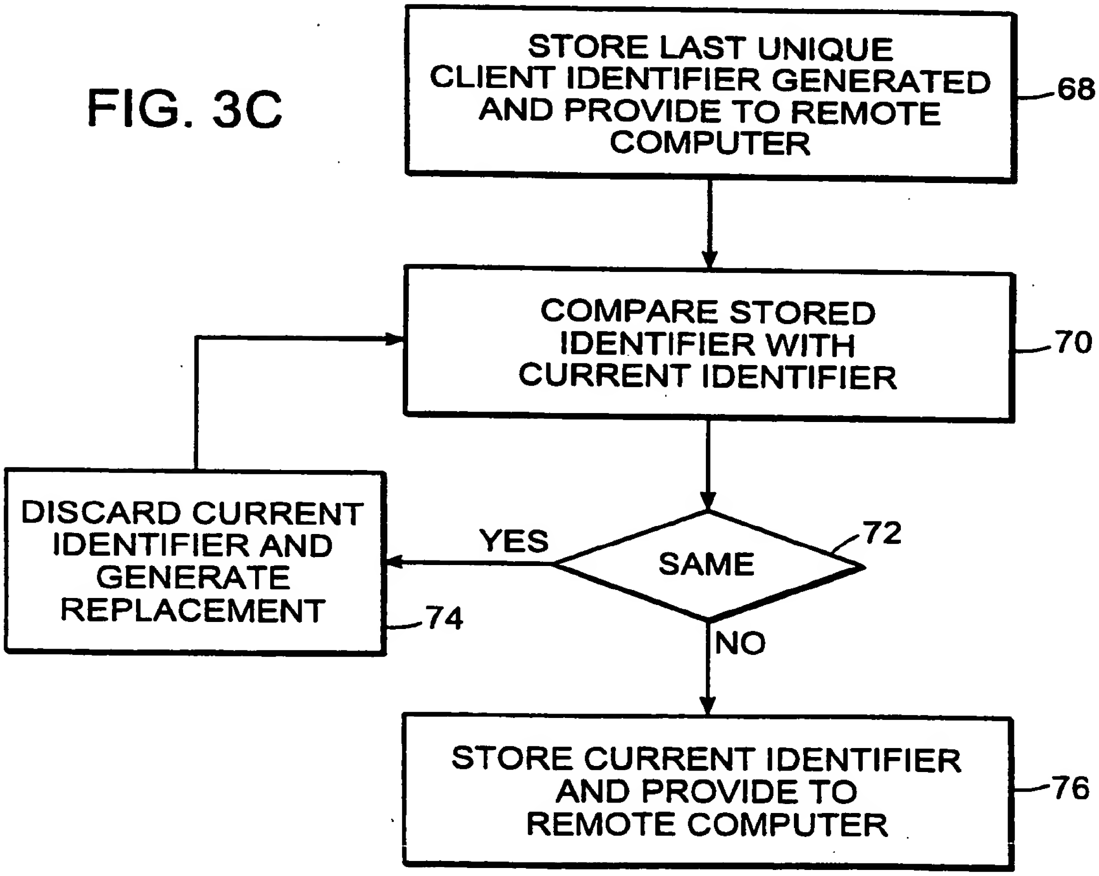

CONCATENATE
HARDWARE-LEVEL (MAC) ADDRESS
AND
CURRENT DATE AND TIME
58
66

FIG. 3C


STORE LAST UNIQUE CLIENT IDENTIFIER GENERATED AND PROVIDE TO REMOTE COMPUTER
68
COMPARE STORED IDENTIFIER WITH CURRENT IDENTIFIER
70
SAME
72
YES
NO
DISCARD CURRENT IDENTIFIER AND GENERATE REPLACEMENT
74
STORE CURRENT IDENTIFIER AND PROVIDE TO REMOTE COMPUTER
76

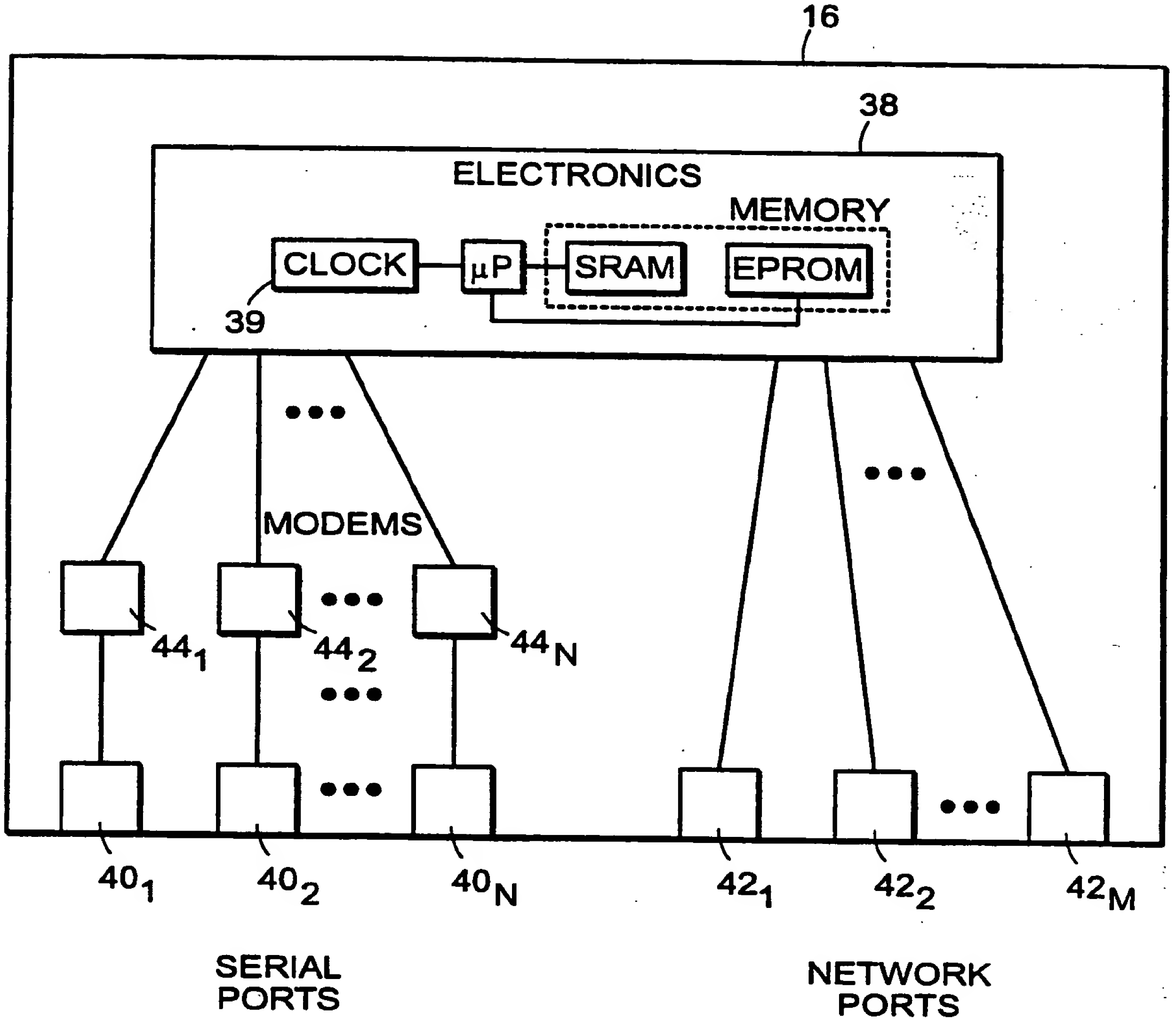

16
38
ELECTRONICS
MEMORY
CLOCK
µP
SRAM
EPROM
39
MODEMS
44_1
44_2
44_N
40_1
40_2
40_N
42_1
42_2
42_M
SERIAL PORTS
NETWORK PORTS

FIG. 4

INTERNATIONAL SEARCH REPORT

Inter   ıal Application No
PCı/US 96/04603

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6   H04L29/06

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6   H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP,A,0 483 547 (IBM) 6 May 1992 see column 3, line 5 - line 54 see column 5, line 12 - column 6, line 22 see column 6, line 51 - column 7, line 7	1-3
Y		7,12,17

Y	EP,A,0 472 836 (IBM) 4 March 1992 see column 9, line 10 - column 11, line 24	7,12,17

□ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search 30 July 1996	Date of mailing of the international search report 0 7. 08. 96
Name and mailing address of the ISA European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+ 31-70) 340-2040, Tx. 31 651 epo nl, Fax (+ 31-70) 340-3016	Authorized officer Canosa Areste, C

1

INTERNATIONAL SEARCH REPORT

Interr ·al Application No
PC1/US 96/04603

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP-A-483547	06-05-92	US-A- 5159592	27-10-92
		DE-D- 69119353	13-06-96
		JP-A- 4227149	17-08-92
EP-A-472836	04-03-92	US-A- 5276813	04-01-94
		JP-A- 4241661	28-08-92
		JP-B- 6056596	27-07-94